Appendix 3:

Data Processing Agreement

This Data Processing Agreement was originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

Data Pro Statement

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

General information

1. This Data Pro Statement has been issued by the following data processor:

   Circel B.V. (hereinafter also referred to as '**Circel**'), Kastanjelaan 400, 5616 LZ Eindhoven, the Netherlands, Chamber of Commerce: 97449075, VAT number: NL868055645B01.

   For questions regarding this Data Pro Statement, please contact Mr. Marco Vogels via marco@circel.com or by phone at +31 6 41774312.

2. This Data Pro Statement is effective as of June 2025.

   We regularly update this Data Pro Statement, and the security measures described herein to ensure continued preparedness and compliance with data protection requirements. We will inform you of new versions via our regular communication channels.

3. This Data Pro Statement applies to all products and services where **Circel** acts as a processor within the meaning of the General Data Protection Regulation (GDPR).

4. Description of products/services.

   Circel is a service provider specialised in delivering IT services related to the open-source ERP platform Odoo. Circel's activities cover the full range from ERP implementation to consulting, support, training, and the development of custom solutions.

   Circel primarily focuses on supporting organisations in setting up and optimising their business processes using Odoo. This includes, among other things:

   - Implementation services: guidance in setting up and configuring Odoo modules tailored to the client's operations;
   - Consulting: functional and technical advice on the use of Odoo within the organisation;
   - Custom development: building custom functionalities, integrations with external systems (APIs, middleware), and reports;
   - Support & maintenance: assistance with incidents, bug fixes, updates, and changes after go-live;
   - Training and knowledge transfer: training of end users and key users in the use of Odoo.

   Circel's services focus on implementation, consulting, and support for the use of Odoo. When clients use Odoo Online or Odoo.sh, hosting and infrastructure are provided by Odoo S.A. Circel does not offer its own hosting environment or SaaS service but operates as an implementation and consulting partner within the existing Odoo ecosystem.

   When performing certain actions within these services – such as importing, exporting, or modifying data on behalf of the client – Circel processes personal data exclusively within the client's Odoo environment and in accordance with the client's instructions. In these cases, Circel acts as a data processor.

   In addition, personal data (such as names and email addresses) may be received by Circel via communication channels such as email or helpdesk portals. Circel processes such data solely in the context of support services and secures it in line with the measures described in this statement.

   Circel never processes personal data for its own purposes and only to the extent necessary to deliver the agreed-upon services. All processing activities are carried out in accordance with the agreements made with the client and within the applicable legal framework.

5. Intended Use.

   Circel supports organisations in the implementation, optimisation, and use of Odoo software. In this context, we

process personal data solely on behalf of the customer and within the scope of the agreed services, such as functional support, custom development, and integrations.

In performing our services, we may have access to personal data entered by the customer into Odoo, including names, business contact details, usernames, log data, and—if present—also private information such as home addresses (for example, through the HR modules).
Processing takes place exclusively for the execution of the assignment or in accordance with the customer's written instructions as the data controller.

Our services are not specifically designed for the processing of special categories of personal data or criminal data. If the customer processes such data within Odoo, this is done at their own responsibility.

6. **Circel** has applied privacy by design/privacy by default in the following manner:

Circel applies the principles of privacy by design and privacy by default within its services, insofar as this is possible within our role as data processor. Personal data is only processed within the customer's Odoo environment, with minimal access and only where necessary for the execution of the agreed assignment.

We do not export or store personal data outside of this environment, unless this has been explicitly and contractually agreed upon with the client.

The responsibility for ensuring privacy by design and privacy by default within the configuration and use of Odoo lies primarily with the client as the data controller. The client independently determines which personal data is entered, processed, and stored in Odoo, and is responsible for correctly configuring authorisations, retention periods, and access rights.

We support clients in implementing these principles by providing best practices, advice on access security, and by limiting data processing to what is functionally necessary.

7. **Circel** uses the Standard Clauses for Processing, which are included below. The Data Pro Statement, together with the Standard Clauses for Processing, constitutes a data processing agreement.

8. **Circel** processes personal data primarily within the EU/EEA. Circel has ensured an appropriate level of protection in the following way:

Personal data is primarily processed within the customer's Odoo environment or within Circel's own Odoo.sh environment, both of which are hosted within the European Union. For supporting communication and office services, Circel also uses Microsoft 365. In this context, personal data may occasionally be processed outside the EU/EEA, for example in connection with email communication or technical support.

Microsoft acts as a data processor and has implemented appropriate safeguards, including Standard Contractual Clauses (SCCs) and participation in the EU–US Data Privacy Framework. These data transfers are strictly limited to what is necessary for the delivery of services and communication with clients.

- Microsoft 365: Circel's data is stored exclusively within the European Union, in accordance with Microsoft's EU Data Boundary program. Datacenters used are located in Dublin (Ireland), Amsterdam (Netherlands), Finland, and Austria. Microsoft provides SCCs and legal guarantees to ensure GDPR compliance.
- Odoo.sh (Odoo S.A.): Circel's internal Odoo.sh environment is hosted in Saint-Ghislain (Belgium), through explicit selection of the EU hosting region. Backups are stored in multiple European datacenters in accordance with Odoo S.A.'s retention policy and remain within the EU.

9. **Circel** uses the following sub-processors in the context of its services. If the processing of personal data, including potentially private data, takes place through these sub-processors, this will occur only if necessary for the execution of the agreement and with the client's consent:

1. Microsoft Ireland Operations Limited
   - Purposes of processing: Email, document management, file storage, collaboration tools (Microsoft 365, including Outlook, Word, Excel, and Teams).
   - Types of personal data: Names, email addresses, project documentation, communication data.
   - Location of processing: Within the EU (Dublin, Amsterdam, Finland, or Austria), in accordance with Microsoft's EU Data Boundary commitment.
   - Legal entity: Ireland (EU).
   - Legal safeguards: Microsoft offers a Data Protection Addendum incorporating Standard Contractual Clauses (SCCs). Customer data remains within the EU/EFTA and is not transferred to third countries.
   - More information: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr
2. Odoo S.A.
   - Purposes of processing: Hosting and processing of data within Circel's Odoo environment, including

project administration, client data, and other business processes.
- Types of personal data: Client data, user data, project information
- Location of processing: Within the EU. For EU-based projects, Circel explicitly selects hosting in Saint-Ghislain (Belgium). Backups are replicated across multiple European data centers in accordance with Odoo.sh's retention policy.
- Legal entity: Belgium (EU).
- Legal safeguards: Odoo processes data exclusively within the EU and complies with GDPR requirements as outlined in its privacy policy.
- More information: https://www.odoo.com/privacy

Circel monitors its sub-processors through annual reviews of their privacy statements, certifications, and compliance documentation. In the event of any change affecting data processing, Circel will proactively inform its clients.

10. **Circel** supports you in the following way with data subject requests:

Circel supports its clients (in their role as data controllers) in handling data subject requests as defined under the General Data Protection Regulation (GDPR). This includes requests for access, rectification, erasure, restriction of processing, or data portability.

Clients can submit such requests via: info@circel.com.

Circel will confirm receipt of the request within one 1 business day and, where reasonably possible, provide support or process the request within 30 calendar days of receiving a complete and valid request.

If a data subject contacts Circel directly, Circel will forward the request to the relevant client without any substantive review or processing. Circel will only act on a data subject request following explicit written instruction from the client. Any costs associated with executing the request will be communicated to the client in advance.

11. **Circel** will cooperate with Data Protection Impact Assessments as follows:

Circel will cooperate in conducting a Data Protection Impact Assessment (DPIA) when required under the GDPR (in particular Articles 35 and 36) and to the extent that it concerns the processing of personal data for which Circel acts as processor.

The procedure is as follows:
- You can contact us by email at info@circel.com.
- Please clearly specify, in a reasonable and detailed request, the type of support you require from Circel in the context of the DPIA.
- Circel will provide the requested assistance as soon as reasonably possible. Additional costs may apply in accordance with our standard hourly rate.

12. After the agreement with a client has ended, Circel will delete the personal data it has processed on behalf of the client within three months, in such a way that the data can no longer be used and has been rendered inaccessible.

13. Deletion or return of personal data upon termination or change of processing

No specific arrangements have been made regarding the return of personal data after termination of the Agreement. If the client submits a request before the applicable data retention period has expired, Circel will assess, in consultation with the client, whether and how the personal data can be returned. Any related costs will be agreed upon in advance.

If a sub-processor is replaced or discontinues its services, Circel will inform the client in a timely manner. Circel will ensure a secure and proper transfer or migration of the data to the new party, in accordance with the requirements of the GDPR. Deletion at the former sub-processor will take place once the migration is complete and any applicable legal retention periods have expired.

Security policy

14. **Circel** has implemented the following security measures to safeguard its product or service:

Circel operates exclusively within customer-managed Odoo environments (such as Odoo Online and Odoo.sh). The technical infrastructure and primary security measures are provided by Odoo S.A. Circel delivers its services within these protected environments and applies the following safeguards to ensure the careful processing of personal data:
- All work is performed within Odoo Online or Odoo.sh, platforms managed by Odoo S.A. and certified with relevant security standards. These environments offer encryption of data in transit and at rest (such as TLS 1.2+ and AES-256).

- Circel also uses its own Odoo.sh environment and Microsoft 365 for internal project administration and documentation. These platforms also encrypt data in transit and at rest, in accordance with their standard security practices.
- Logging takes place at the platform level within Odoo.sh and Microsoft 365, to the extent these functionalities are offered by the platforms.
- Circel limits access to client data to only those employees who strictly need it, depending on the assignment or client request.
- All employees of Circel are bound by confidentiality obligations.
- Upon termination of employment, user accounts are immediately deactivated and access to client data is revoked.
- Two-factor authentication is used where possible.
- No client data is stored locally on laptops or external drives; all data processing takes place within secured cloud platforms.
- Pseudonymisation is not applied by default. If desired, this can be configured upon request within the client's own Odoo environment (for example, via custom fields or reports with masked data).
- Confidentiality, integrity, availability, and resilience are ensured through access control, secure infrastructure, and minimisation of access.
- Incident recovery: Circel works together with the client and Odoo S.A. to restore access to personal data in a timely manner in case of incidents. Circel immediately informs clients of any incident that impacts its access or processing.

Backups of client environments are managed exclusively by Odoo S.A.; Circel does not have an active or additional backup role in this. Circel also uses backups of its own internal systems (such as its internal Odoo environment) via Odoo.sh. For Circel, backups are automatically created and replicated across multiple European data centers — with EU configuration this is in Saint Ghislain (Belgium). Backups are created daily and stored according to Odoo.sh's retention policy:

- 7 daily backups,
- 4 weekly backups,
- 3 monthly backups.

Circel does not conduct its own penetration tests, as client data is exclusively hosted via Odoo.sh and Microsoft 365, both of which are subject to regular external audits and penetration testing.

15. **Circel** has not yet formally aligned to the Information Security Management System (ISMS):

Circel strives to align as much as possible with the standards of ISO 27001 and intends to fully comply with this information security standard in the future. In addition, the guidelines of ISMS NLdigital are followed, insofar as they are relevant to the services provided by Circel.

16. **Circel** has the following certifications:

- Circel holds the Odoo V18 Certificate and is officially accredited as an Odoo Partner.
- Circel is actively working toward obtaining additional certifications, including ISO 27001 and the Data Pro Certificate from Scope Europe, once these processes have been completed.

Data Breach Protocol

17. What does **Circel** do in case something goes wrong, and a data breach occurs:

In the unfortunate event that something goes wrong, Circel applies the following data breach protocol to ensure that you, as the client, are informed in a timely and adequate manner about any security incidents involving personal data processed on your behalf:

- You, as the data controller, are responsible for notifying the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) and, if applicable, the data subjects, in accordance with Articles 33 and 34 of the GDPR.
- Circel will inform you without undue delay as soon as we become aware of an incident that (potentially) concerns personal data processed on your behalf.
- The notification will be sent via email to the contact person designated by you. If no specific contact has been provided, Circel will use the primary contact address known to us. You are kindly requested to inform us in writing of the appropriate contact person.
- The notification will include, where reasonably possible at the time:
    1. A summary of the security incident.
    2. Information about the nature and scope of the incident, including (if known) the categories of personal data and data subjects affected.
    3. The nature of the breach (e.g., loss, unauthorised access, modification, or disclosure).
    4. The suspected cause of the incident.
    5. Mitigation measures already taken and/or planned.
    6. An assessment of the risks to the rights and freedoms of data subjects.
    7. Information about the affected systems or components of our services.
- Where reasonably possible, Circel will assist in providing additional information required to meet

your legal notification obligations. Any reasonable costs for such support will be agreed with you in advance.

- In the event of incidents at sub-processors, you will be informed as soon as Circel has been notified

Standard Clauses for Data Processing

Version: March 2025

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.
1.2 **GDPR:** the General Data Protection Regulation.
1.3 **Data Processor**: the party which, in their capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.
1.4 **Data Pro Statement**: a statement issued by the Data Processor in which they provides information such as the intended use of its products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.
1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.
1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.
1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.
1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor as required under the Agreement.
1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing, which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General Provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.
2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.
2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written instructions provided by Client and accepted by Data Processor.
2.4 Client or their customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.
2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data and shall not make any decisions on the use of the Personal Data and other such matters.
2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.
2.7 Client shall guarantee Data Processor that they act in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.
2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in their Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of their products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.
3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data

Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures they shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures they has implemented if to its discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments they choose to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honor such requests to adjust their security measures. If Data Processor makes any adjustments to its security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing.

Article 4. Data breaches

4.1 Data Processor does not guarantee that their security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, they shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or their customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or their customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet their breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, they are entitled to invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6. Term and Termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, they shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of their statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The Rights of Data Subjects, Data Protection Impact Assessment (DPIA) and Auditing Rights

7.1 Data Processor, were possible, shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, they shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor will lend their cooperation to Client's requests for the deletion of personal data insofar as Client cannot carry this out themself.

7.4 Data Processor shall be able to demonstrate its compliance with their requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third- party memorandum) issued by an independent expert.

7.5 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at its own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with their obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to their discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.

7.6 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to their discretion such are appropriate, taking into account the processing risks associated with their product or service, the state of the art, the costs of implementation, the market in which they operate, and the intended use of the product or service.

7.7 Data Processor shall be entitled to invoice Client for any costs they incur in implementing the measures referred to in this article.

Article 8. Sub-Processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (sub processors) to help them process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet its obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes. Data Processor shall ensure that any third parties they hire shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other Provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.